

ABSTRACT OF THE DISCLOSURE

This invention intends to reduce the amount of calculation required by a cipher strength estimating device for estimating a ciphertext in collectively finding session keys for plural rounds of transformation. The cipher strength estimating device is configured to: first calculate one session key prospect presumed to be equivalent to a session key for use at a certain round of transformation in encryption which is calculated from a key; perform a decrypting operation with the session key prospect presumed to be true; calculating a session key prospect for the round immediately preceding the certain round based on the resulting text thereby calculating session keys for different rounds. This device enhances the possibility that plural true session keys are calculated faster.

Fig. 1

1...CONTROL UNIT, 2...PUTATIVE TRANSFORMED TEXT, 3...PUTATIVE UNTRANSFORMED TEXT CALCULATING UNIT, 4...RECALCULATION REQUEST DATA, 5...PLAINTEXT, 6...PUTATIVE UNTRANSFORMED TEXT CALCULATING UNIT, 7...SESSION KEY PROSPECT, 8...SESSION KEY PROSPECT CALCULATING SECTION, 9...UNCALCULABILITY IDENTIFIER DATA, 10...PUTATIVE UNTRANSFORMED TEXT

Fig. 2

1...CIPHERTEXT OR PUTATIVE UNTRANSFORMED TEXT, 2...FIRST PUTATIVE UNTRANSFORMED TEXT CALCULATING SECTION, 3...PUTATIVE UNTRANSFORMED TEXT CALCULATING UNIT BODY, 4...FIRST SESSION KEY PROSPECT CALCULATING SECTION

Fig. 3

101...CPU, 102...INTERNAL MEMORY, 103...EXTERNAL STORAGE UNIT, 104...COMMUNICATION INTERFACE, 105...DISPLAY, 106...INPUT MEANS,

Fig. 4

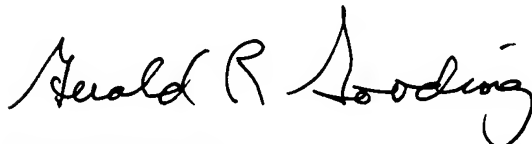
3...PLAINTEXT AND CIPHERTEXT CALCULATING UNIT

I, Gerald R. Gooding, of 5191 Meadowlark Drive, Huntington Beach, California, do hereby certify that the identified portions of the Japanese original that bear a circled number (2) through (17) and my hand-written initials (AG) correspond to the similarly numbered and underlined portions of the English translation above that bear my hand-written initials as described below. Specifically, I certify that:

- * (2) on page 3/21 line 1 of the Japanese original corresponds to the underlined portion (2) on page 3 line 26 to page 4 line 2 of the above English translation.
- * (3) on page 4/21 line 1 of the Japanese original corresponds to the underlined portions (3a-3c) on page 6 lines 1 to 8 of the above English translation.
- * (4) on page 5/21 line 1 of the Japanese original corresponds to the underlined portions (4a-4d) on page 8 lines 3 to 10 of the above English translation.
- * (5) on page 6/21 line 1 of the Japanese original corresponds to the underlined portion (5) on page 10 lines 9 to 10 of the above English translation.
- * (6) on page 7/21 line 1 of the Japanese original corresponds to the underlined portions (6a-6b) on page 12 lines 12 to 14 of the above English translation.
- * (7) on page 8/21 line 1 of the Japanese original corresponds to the underlined portion (7a-7b) on page 14 lines 20 to 23 of the above English translation.
- * (8) on page 9/21 line 1 of the Japanese original corresponds to the underlined portion (8) on page 16 lines 1 to 2 of the above English translation.
- * (9) on page 10/21 line 1 of the Japanese original corresponds to the underlined portion (9) on page 17 line 20 of the above English translation.
- * (10) on page 11/21 line 1 of the Japanese original corresponds to the underlined portions (10a-10b) on page 19 lines 18 to 19 of the above English translation.
- * (11) on page 13/21 line 1 of the Japanese original corresponds to the underlined portions (11) on page 22 lines 11 to 15 of the above English translation.

- * (12) on page 14/21 line 1 of the Japanese original corresponds to the underlined portions (12a-12c) on page 24 lines 13 to 18 of the above English translation.
- * (13) on page 15/21 line 1 of the Japanese original corresponds to the underlined portion (13) on page 26 lines 21 to 23 of the above English translation.
- * (14) on page 17/21 line 1 of the Japanese original corresponds to the underlined portions (14a-14b) on page 28 line 2 and page 30 lines 1 to 2 of the above English translation.
- * (15) on page 18/21 line 1 of the Japanese original corresponds to the underlined portions (15a-15b) on page 30 line 5 and page 32 lines 6 to 7 of the above English translation.
- * (16) on page 19/21 line 1 of the Japanese original corresponds to the underlined portions (16a-16c) on page 34 lines 11 to 14 of the above English translation.
- * (17) on page 20/21 line 1 of the Japanese original corresponds to the underlined portions (17a-17b) on page 36 lines 11 to 14 of the above English translation.

I further certify that I am accredited for Japanese-to-English translation by the American Translators Association (225 Reinekers Lane, Suite 590, Alexandria, VA 22314, Tel. 703.683-6122), effective 28 December 1989.

 16 Jan 2004
Gerald R. Gooding
